# LES DONNÉES DE SANTÉ : UNE PROTECTION NÉCESSAIRE

## Hébergement des données de santé : les premiers hébergeurs sont agréés

**La procédure d'agrément ministériel des hébergeurs de données de santé a repris le 2 février 2009 après une suspension de deux ans. La Commission s'est prononcée sur les dossiers de candidature qui lui ont été adressés par la ministre de la Santé après s'être assurée du déploiement par les candidats hébergeurs de solutions de sécurité effectives et de haut niveau et de l'exercice effectif des droits des patients.**

À l'heure où le partage des données de santé entre un nombre croissant d'acteurs du système de soins est reconnu par tous comme contribuant à l'amélioration de la qualité des soins et à la maîtrise des dépenses, le développement de l'e-santé est inéluctable. Dans ce contexte, la sécurité des données personnelles de santé est une priorité renforcée.

La procédure d'agrément des hébergeurs de données de santé à caractère personnel, instaurée par la loi du 4 mai 2002 relative aux droits des malades, vise à garantir la sécurité des données personnelles de santé lorsqu'elles sont hébergées par un organisme distinct du professionnel ou de l'établissement de santé qui soigne le malade.

Les conditions de l'agrément ont été fixées par le décret du 4 janvier 2006 qui organise la procédure d'agrément et fixe le contenu du dossier qui doit être fourni à l'appui de la demande.

Cet agrément est délivré pour une durée de trois ans par le ministre chargé de la Santé, qui se prononce après avis de la CNIL et du Comité d'agrément créé auprès de lui.

Cette procédure particulière et préalable s'applique sans préjudice des formalités propres à la loi « Informatique et Libertés », auxquelles restent soumis les professionnels et établissements de santé, qui, en leur qualité de responsables de traitements automatisés de données à caractère personnel, font héberger leurs bases de données chez des organismes agréés.

En raison notamment de la lourdeur de la procédure et du grand nombre d'applications susceptibles d'être concernées, la loi du 30 janvier 2007 a suspendu, sauf lorsqu'il s'agit d'héberger des dossiers médicaux personnels, la procédure d'agrément pendant deux ans à compter du 2 février 2007, le temps, pour le comité, d'élaborer les référentiels nécessaires à l'instruction des dossiers.

Ce référentiel, destiné à permettre une autoévaluation par les candidats et un traitement efficace des demandes d'agrément, a été élaboré par l'Agence des systèmes d'information partagés de santé (ASIP Santé, anciennement dénommée GIP-DMP), en concertation avec les industriels. La CNIL a été associée à la définition de ce référentiel. Elle est également associée aux réunions du Comité d'agrément des hébergeurs.

Les premières décisions de la ministre sont intervenues et devraient être publiées en mars 2010. En dehors des agréments délivrés en 2006 dans le cadre de l'expérimentation du DMP pour le temps de l'expérimentation, les premiers hébergeurs de données de santé seront donc agréés.

# Quel calendrier pour le DMP?

Le projet initial a donné lieu à de nombreux rapports sur la conduite du projet qui ont guidé les orientations d'un programme de relance du projet. L'idée maîtresse de ce programme est d'inscrire le projet DMP dans une stratégie de développement des systèmes d'information de santé.

Une nouvelle Agence des systèmes d'information de santé partagés (ASIP) a été mise en place et regroupe le GIP-DMP, le GIP-CPS (carte de professionnel de santé) et le département « interopérabilité » du GMSIH (Groupement pour la modernisation du système d'information hospitalier). Cette agence est chargée de relancer le projet DMP et d'*« élaborer des normes d'interopérabilité et de sécurité des systèmes d'information »* de santé en général.

Le projet, orienté sur la notion de services rendus aux usagers du système de santé et aux professionnels de santé, devrait être développé en deux étapes :

**• La première étape: 2009 à 2012**

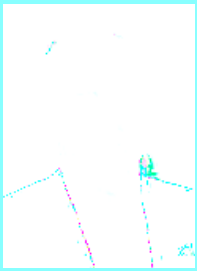
Il s'agit d'une phase d'expérimentation au cours de laquelle un dossier patient « socle » sera déployé au niveau national et alimenté notamment par les comptes rendus de consultation et d'hospitalisation. Parallèlement, les conditions du développement des systèmes d'informations partagées seront précisées (concertation avec les acteurs concernés, développement de l'usage de la carte de professionnel de santé (CPS) dans les établissements, mise en convergence des projets territoriaux, production de référentiels d'interopérabilité et de sécurité).

**• La deuxième étape: à partir de 2012**

Un portail unique sera mis en place permettant le déploiement complet du DMP.

La loi nº 2009-879 du 21 juillet 2009 portant réforme de l'hôpital, relative aux patients, à la santé et aux territoires (dite « HPST ») a consacré le caractère facultatif du DMP et supprimé la sanction de moindre remboursement en cas de refus d'accès du patient.

## Questions à ...



### Jean Massot

*Président de section honoraire au Conseil d'État*
*Commissaire en charge du secteur « Santé et assurance maladie »*

***Quel est le rôle de la CNIL dans ce dispositif?***

En sa qualité d'autorité de protection des données personnelles, la CNIL a accompagné toutes les phases de définition et de réalisation du dossier médical personnel.
Elle devra encore se prononcer sur un certain nombre de textes qui commandent la généralisation du dispositif (décret DMP, décret identifiant) et autoriser les différentes phases de développement du projet.
À diverses reprises, la Commission a eu l'occasion de rappeler les conditions qui, de son point de vue, sont nécessaires pour mener à bien ce projet.
Outre la définition d'un cadre juridique stable déjà évoquée, le déploiement de solutions de sécurité effectives et de haut niveau est nécessaire. Seul un contexte de sécurité garantie sera de nature à permettre un exercice effectif des droits des patients prévus par la loi. La modernisation des systèmes d'information des professionnels de santé est donc un préalable à la poursuite du projet.
La CNIL porte une attention particulière à l'effectivité des droits des patients, notamment en matière de recueil du consentement explicite et exprès. Conformément aux dispositions de la loi du 6 janvier 1978, l'information délivrée au patient sur ses droits doit être claire, complète et préalable sur les finalités et fonctionnalités du DMP.
En outre, la CNIL souhaite une harmonisation des régimes juridiques, et en particulier des modalités de consentement du patient à l'ouverture ou à l'accès des différents dossiers de santé sur internet (dossier pharmaceutique, dossier de cancérologie, dossier de réseaux de soins).
La CNIL est associée au groupe de travail qui a été constitué en 2009 et dont l'objectif est de produire un guide de bonnes pratiques sur les modalités de recueil du consentement des patients et l'utilisation par les professionnels de santé des données de santé à caractère personnel.
Un équilibre est à trouver entre les besoins des professionnels de santé et ceux des patients dont l'implication est indispensable. La CNIL ne peut trouver que des avantages à voir renforcés les voies et les moyens d'une coopération régulière entre les différents acteurs sur le sujet des dossiers médicaux électroniques et de la protection des données personnelles de santé.

## L'anonymisation : une condition d'accès des complémentaires aux données de santé

**La Commission nationale de l'informatique et des libertés a autorisé le 10 décembre 2009, la Mutualité française, les sociétés Axa-France et GROUPAMA, à prolonger les expérimentations ayant pour finalité de recourir et d'exploiter, sous forme anonymisée, les données de santé figurant sur les feuilles de soins électroniques.**

En décembre 2009, elle a autorisé, pour une durée de trente-six mois, la poursuite de ces expérimentations après avoir analysé les bilans des complémentaires santé qui en avaient fait la demande. Les expérimentations ont toutes pour objet de permettre la transmission aux organismes d'assurance-maladie complémentaire (AMC) des codes des médicaments et en matière d'optique des codes produits et prestations délivrées à l'assuré. L'accès à ces données qui figurent sur les feuilles de soins électroniques permet aux complémentaires de mieux identifier les soins remboursés et ainsi de simuler ou de proposer à leurs assurés des garanties contractuelles modulées, d'affiner leur tarification sur la prise en charge de spécialités non remboursées par le régime obligatoire et d'inciter les assurés à adhérer à des actions de prévention. Alors que la politique du gouvernement vise à diminuer ou à dérembourser certains produits ou prestations à service médical rendu estimé insuffisant, l'accès apparaît pour les AMC d'autant plus nécessaire qu'elles souhaitent jouer un rôle accru en matière de maîtrise des dépenses de santé.

Afin de s'assurer que les données qui pourraient conduire à identifier les assurés ne viennent à la connaissance des AMC tout en permettant à ceux-ci d'affiner les garanties qu'ils proposent, la Commission a demandé que l'anonymisation repose sur l'utilisation d'une boîte noire, c'est-à-dire un dispositif matériel inviolable même par les complémentaires santé, audité par un organisme extérieur à l'AMC.

La CNIL a également donné son aval sur un dispositif technique proposé par le ministère de la Santé en concertation avec les différents acteurs du secteur qui permettra, dans le cadre de SESAM Vitale, de transmettre des données détaillées des feuilles de soins électroniques (FSE) vers les serveurs des organismes complémentaires. Cette solution définit des règles de sécurité pour les échanges de données de santé (FSE) entre le professionnel de santé et les complémentaires santé. Les AMC disposent de trois ans pour se mettre en conformité avec ce dispositif.

La CNIL a donc autorisé les trois organismes d'AMC, qui en ont fait la demande, à poursuivre les expérimentations en cours, en les invitant à adopter, dans l'intervalle, l'architecture commune proposée par le ministère.

L'audit du système par un organisme extérieur et la mise en conformité avec la solution générique d'acheminement des données de santé sont des points indispensables avant toute généralisation. Les trois organismes d'AMC devront, au terme de la période de trois ans, présenter une nouvelle demande d'autorisation et soumettre, à l'appui de la demande la nouvelle architecture d'acheminement des données adoptée dans leurs systèmes d'information.

Toutefois, la Commission continue d'appeler de ses vœux une loi qui définisse les données de santé pouvant être transmises aux AMC, les garanties appropriées et les conditions de transmission de ces données.

### La CNIL explique

**L'anonymisation**

La CNIL peut autoriser des applications comportant des informations sensibles, telles que les données de santé, dès lors que celles-ci font l'objet « à bref délai » d'un procédé d'anonymisation reconnu conforme à la loi.
Depuis de nombreuses années, la CNIL préconise le recours à de telles techniques d'anonymisation notamment dans le domaine statistique. De tels procédés ont ainsi été employés dans des domaines aussi divers que la surveillance sanitaire (déclarations obligatoires du sida), les statistiques d'activité hospitalières (PMSI), le système national d'information sur l'assurance-maladie ou encore les transports (analyse anonyme des trajets avec la carte NAVIGO dans la région parisienne).

Dans le cadre des demandes de prêts, en particulier immobiliers, les emprunteurs ont l'obligation de souscrire une assurance qui garantit à la banque le remboursement du crédit en cas de décès ou de maladie. Ces contrats se concluent auprès de compagnies d'assurance qui sont amenées, à cette occasion, à collecter de nombreuses données de santé concernant les demandeurs de crédit.

L'enjeu des traitements mis en œuvre, tant au regard du nombre de personnes concernées que de la nature des données traitées, nécessite que la loi « Informatique et Libertés » soit rigoureusement respectée. La Commission a donc effectué plus d'une quinzaine de contrôles auprès de compagnies d'assurance, de cabinets de courtage en assurance et du bureau commun d'assurances collectives (BCAC).

La CNIL a constaté que les sociétés d'assurance ne procédaient pas à une mutualisation ou à un échange d'informations concernant la santé des personnes. Toutefois, elle a relevé d'importants manquements à la loi « Informatique et Libertés », portant notamment sur la confidentialité, la sécurité et la durée de conservation des données de santé. En effet, ces informations sensibles sont souvent accessibles à un très grand nombre de salariés au sein des compagnies d'assurance (service informatique, service clientèle, etc. ). De surcroît, les dossiers contenant des données de santé sont parfois examinés par des services qui ne sont pas placés sous la responsabilité des médecins conseils. Les contrôles ont mis également en évidence l'insuffisance globale des mesures de sécurité apportées aux données de santé, en particulier leur absence de chiffrement. Par ailleurs, de nombreuses compagnies d'assurance conservent de manière excessive des informations de santé, en particulier sur des personnes qu'elles n'assurent pas ou plus. Enfin, lorsqu'une personne exerce son droit d'accès, les informations la concernant détenues par l'assureur ne lui sont pas toujours communiquées en intégralité.